X.509 Certificate Policy
for the

U.S. Federal PKI
Common Policy Framework

Version 2.5 **16 October 2006**

Revision History

Document Version	Document Date	Revision Details
2.0	01 November 2004	This Common Policy CP updates and replaces Version 1.4, dated 10 February 2004. Text changes are specified in the following Common Policy CP Change Proposals (**change proposal number**, title, date): **2004-01**, Common Policy Modifications and Clarifications, 8 June 2004
2.1	09 February 2005	This Common Policy CP updates and replaces Version 2.0, dated 01 November 2004. Text changes are specified in the following Common Policy CP Change Proposals (**change proposal number**, title, date): **2005-01**, Common Policy Modifications to Support FIPS 201, 14 January 2005
2.2	29 March 2005	This Common Policy CP updates and replaces Version 2.1, dated 09 February 2005. Text changes are specified in the following Common Policy CP Change Proposals (**change proposal number**, title, date): **2005-02**, Common Policy Modifications to Support FIPS 201, 21 March 2005
2.3	19 September 2005	This Common Policy CP updates and replaces Version 2.2, dated 29 March 2005. Text changes are specified in the following Common Policy CP Change Proposals (**change proposal number**, title, date): **2005-03**, Addition of High Assurance Policy to the Common Policy Framework, 13 September 2005
2.4	15 February 2006	This Common Policy CP updates and replaces Version 2.3, dated 19 September 2005. Text changes are specified in the following Common Policy CP Change Proposal (**change proposal number**, title, date): **2006-01**, Alignment of Common Authentication Policies with FIPS 201, 30 January 2006

Document Version	**Document Date**	**Revision Details**
2.5	16 October 2006	This Common Policy CP updates and replaces Version 2.4, dated 15 February 2006. Text changes are specified in the following Common Policy CP Change Proposals (**change proposal number**, title, date): **2006-02**, Accelerated adoption of changes in draft RFC 3647 version of policy, 10 October 2006

FOREWORD

This is the policy framework governing the public key infrastructure (PKI) component of the Federal Enterprise Architecture. The policy framework incorporates six specific certificate policies: a policy for users with software cryptographic modules, a policy for users with hardware cryptographic modules, a policy for devices, a high assurance user policy, a user authentication policy, and a card authentication policy.

The user policies apply to Federal employees, contractors and other affiliated personnel requiring PKI credentials for access to Federal systems that have not been designated by law as national security systems. The device policy applies to devices operated by or on behalf of federal agencies. These policies may be used by PKIs whose Certification Practice Statement (CPS) and Compliance Audit have been approved by the Federal PKI Policy Authority (PA). Such PKIs may be agency operated or may be operated by approved providers.

This policy framework supports hierarchical PKI, mesh PKI, and single certification authority (CA) implementations of this certificate policy. As such, constraints are established for the secure distribution of self-signed certificates for use as trust anchors. These constraints apply only to CAs that choose to distribute self-signed certificates.

This policy framework requires the use of FIPS 140 validated cryptographic modules by Federal employees, contractors and other affiliated personnel for all cryptographic operations and the protection of trusted public keys. Software and hardware cryptographic mechanisms are equally acceptable under this policy framework. The policy for users with hardware cryptographic modules mandates a Level 2 validation.

This policy framework requires the use of either 2048 bit RSA keys or 224 bit elliptic curve keys along with the SHA-224 and the SHA-256 hash algorithms. CAs are required to use 2048 bit RSA keys or 224 bit elliptic curve keys when signing certificates and CRLs that expire on or after December 31, 2008. CAs are required to use SHA-224 or SHA-256 when signing certificates and CRLs issued on or after January 1, 2009. All subscriber keys in certificates that expire on or after December 31, 2008 must be at least 2048 bit RSA keys or 224 bit elliptic curve keys.

The certificate policies that comprise this policy framework are consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 2527, Certificate Policy and Certification Practice Statement Framework.

The terms and provisions of these Certificate Policies shall be interpreted under and governed by applicable Federal law.

Table of Contents

1. INTRODUCTION

A Public Key Infrastructure (PKI) consists of products and services that provide and manage X.509 certificates for public key cryptography. In general, certificates identify the individual named in the certificate and bind that person to a particular public/private key pair. A certificate policy describes the policies and procedures that are used to verify the binding before certificates are issued, and the maintenance of that binding.

This Certificate Policy (CP) includes six distinct certificate policies: a policy for users with software cryptographic modules, a policy for users with hardware cryptographic modules, a policy for devices, a high assurance user policy, a user authentication policy, and a card authentication policy. Where a specific policy is not stated, the policies and procedures in this specification apply equally to all six policies.

The user policies apply to certificates issued to Federal employees, contractors and other affiliated personnel for the purposes of authentication, signature, and confidentiality. This CP was explicitly designed to support access to Federal systems that have not been designated national security systems.

A PKI that uses this CP will provide the following security management services:

- Key generation/storage
- Certificate generation, update, renewal, rekey, and distribution
- Certificate revocation list (CRL) generation and distribution
- Directory management of certificate related items
- Certificate token initialization/programming/management
- System management functions (e.g., security audit, configuration management, archive.)

The user policies require Federal employees, contractors and other affiliated personnel to use FIPS 140 validated cryptographic modules for cryptographic operations and the protection of trusted public keys. The device policy also requires use of FIPS 140 validated cryptographic modules for cryptographic operations and the protection of trusted public keys.

This policy does not presume any particular PKI architecture. The policy may be implemented through a hierarchical PKI, mesh PKI, or a single certification authority (CA). Any CA that asserts this policy in certificates must obtain prior approval from the Federal PKI Policy Authority.

This policy establishes requirements for the secure distribution of self-signed certificates for use as trust anchors. These constraints apply only to CAs that choose to distribute self-signed certificates, such as a hierarchical PKI's root CA.

This CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) request for comments (RFC) 2527, CP and Certification Practice Statement Framework.

1.1 OVERVIEW

1.1.1 Certificate Policy

Certificates issued under this policy contain a registered certificate policy object identifier (OID), which may be used by a relying party to decide whether a certificate is trusted for a particular purpose. This CP applies only to CAs owned by or operated on behalf of the Federal government that issue certificates according to this policy.

1.1.2 Relationship Between the CP and the CPS

This CP states what assurance can be placed in a certificate issued by the CA. The Certificate Practice Statement (CPS) states how the CA establishes that assurance. Each CA that issues certificates under this CP shall have a corresponding CPS.

1.1.3 Scope

This CP applies to certificates issued to CAs, devices, and Federal employees, contractors and other affiliated personnel. This CP does not apply to certificates issued to groups of people.

1.1.4 Interoperation with CAs Issuing under Different Policies

Interoperation with CAs that issue under different policies will be achieved through policy mapping and cross-certification through the Federal Bridge Certification Authority.

Note that interoperability may also be achieved through other means, such as trust lists, to meet local requirements.

1.2 IDENTIFICATION

This CP provides substantial assurance concerning identity of certificate subjects. Certificates issued in accordance with this CP shall assert at least one of the following OIDs in the certificate policy extension:

id-fpki-common-policy ::= {2 16 840 1 101 3 2 1 3 6}

id-fpki-common-hardware ::= {2 16 840 1 101 3 2 1 3 7}

id-fpki-common-devices ::= {2 16 840 1 101 3 2 1 3 8}

id-fpki-common-authentication ::= {2 16 840 1 101 3 2 1 3 13}

id-fpki-common-High ::= {2 16 840 1 101 3 2 1 3 16}

id-fpki-common-cardAuth ::= {2 16 840 1 101 3 2 1 3 17}

Certificates issued to CAs may contain any or all of these OIDs. Certificates issued to users to support digitally signed documents or key management may contain either the id-fpki-common-policy, id-fpki-common-hardware, or id-fpki-common-High. Certificates issued to devices under this policy include the id-fpki-common-devices.

Certificates issued to users supporting authentication but not digital signature may contain id-fpki-common-authentication. Certificates issued to users supporting authentication where the private key can be used without user authentication may contain id-fpki-common-cardAuth.

1.3 COMMUNITY AND APPLICABILITY

The following are roles relevant to the administration and operation of CAs under this policy.

1.3.1 PKI Authorities

1.3.1.1 PKI Policy Authority

The Federal PKI Policy Authority (PA) is a group of U.S. Federal Government Agencies (including cabinet-level Departments) established by the Federal CIO Council. The PA is responsible maintaining this policy, approving the CPS for each CA that issues certificates under this policy, and approval of the compliance audit report for each CA issuing certificates under this policy.

1.3.1.2 Agency Policy Management Authority

Agencies that operate a CA under this policy, or contract for the services of a CA under this policy, shall establish a management body to manage any agency-operated components (e.g., RAs or repositories) and resolve name space collisions. (see Section 3.1.5). This body shall be referred to as an Agency Policy Management Authority, or Agency PMA.

1.3.1.3 Certification Authority

The CA is the collection of hardware, software and operating personnel that create, sign, and issue public key certificates to subscribers. The CA is responsible for the issuing and managing certificates including—

- The certificate manufacturing process
- Publication of certificates
- Revocation of certificates
- Generation and destruction of CA signing keys
- Ensuring that all aspects of the CA services, operations, and infrastructure related to certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

1.3.1.4 Registration Authority

The registration authority (RA) is the entity that collects and verifies each subscriber’s identity and information that are to be entered into the subscriber’s public key certificate. The RA performs its function in accordance with a CPS approved by the PA. The RA is responsible for—

- Control over the registration process

- The identification and authentication process

1.3.1.5 Related Authorities

The CAs and RAs operating under this CP may require the services of other security, community, and application authorities, such as compliance auditors and attribute authorities. The CPS will identify the parties responsible for providing such services, and the mechanisms used to support these services.

1.3.1.6 Trusted Agent

The trusted agent is a person who satisfies all the trustworthiness requirements for an RA and who performs identity proofing as a proxy for the RA. The trusted agent records information from and verifies biometrics (e.g., photographs) on presented credentials for applicants who cannot appear in person at an RA. The CPS will identify the parties responsible for providing such services, and the mechanisms for determining their trustworthiness.

1.3.2 End Entities

1.3.2.1 Subscribers

A subscriber is the entity whose name appears as the subject in a certificate. The subscriber asserts that he or she uses the key and certificate in accordance with the certificate policy asserted in the certificate, and does not issue certificates. For this policy, subscribers are limited to Federal employees, contractors and affiliated personnel. CAs are sometimes technically considered “subscribers” in a PKI. However, the term “subscriber” as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information.

1.3.2.2 Relying Parties

A relying party is the entity that relies on the validity of the binding of the subscriber’s name to a public key. The relying party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The relying party can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate. A relying party may use information in the certificate (such as CP identifiers) to determine the suitability of the certificate for a particular use.

For this certificate policy, the relying party may be any entity that wishes to validate the binding of a public key to the name of a federal employee, contractor, or other affiliated personnel.

1.3.3 Applicability

The sensitivity of the information processed or protected using certificates issued by the CA will vary significantly. Organizations must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each organization for each application and is not controlled by this CP.

This CP is intended to support the use of validated public keys to access Federal systems that have not been designated national security systems. While a validated public key is not generally sufficient to grant access the key may be sufficient when supplemented by appropriate authorization mechanisms. Credentials issued under this CP may also be used for key establishment. This policy is intended to support applications involving unclassified information, which can include sensitive unclassified data protected pursuant to federal statues and regulations.

Credentials issued under the id-fpki-common-policy policy are intended to meet the requirements for Level 3 authentication, as defined by the OMB E-Authentication Guidance. [E-Auth] Credentials issued under the id-fpki-common-hardware, id-fpki-common-authentication, and id-fpki-common-High policies meet the requirements for Level 4 authentication, as defined by the OMB E-Authentication Guidance. [E-Auth]

In addition this policy may support signature and confidentiality requirements for Federal government processes.

1.4 CONTACT DETAILS

1.4.1 Specification Administration Organization

The PA is responsible for all aspects of this CP.

1.4.2 Contact Person

Questions regarding this CP shall be directed to the Chair of the Federal PKI Policy Authority, whose address can be found at http://www.cio.gov/fpkipa.

1.4.3 Person Determining CPS Suitability for the Policy

The PA shall approve the CPS for each CA that issues certificates under this policy. Reference Section 8.3, CPS Approval Procedures.

2. GENERAL PROVISIONS

2.1 OBLIGATIONS

2.1.1 PA Obligations

The PA shall—

- Approve the CPS for each CA that issues certificates under this policy;
- Review periodic compliance audits to ensure that CAs are operating in compliance with their approved CPSes;
- Review name space control procedures to ensure that distinguished names are uniquely assigned for all certificates issued under this CP;
- Revise this CP to maintain the level of assurance and operational practicality;
- Publicly distribute this CP; and
- Coordinate modifications to this CP to ensure continued compliance by CAs operating under approved CPSes.

2.1.2 Agency PMA Obligations

The Agency PMA shall—

- Review periodic compliance audits to ensure that RAs and other components operated by the agency are operating in compliance with their approved CPSes; and
- Review name space control procedures to ensure that distinguished names are uniquely assigned within their agency.

2.1.3 CA Obligations

A CA who issues certificates that assert a policy defined in this document shall conform to the stipulations of this document, including—

- Providing to the PA a CPS, as well as any subsequent changes, for conformance assessment.
- Maintaining its operations in conformance to the stipulations of the approved CPS.
- Ensuring that registration information is accepted only from approved RAs operating under an approved CPS.
- Including only valid and appropriate information in certificates, and maintaining evidence that due diligence was exercised in validating the information contained in the certificates.
- Revoking the certificates of subscribers found to have acted in a manner counter to their obligations in accordance with Section 2.1.4.
- Operating or providing for the services of an online repository that satisfies the obligations under Section 2.1.5, and informing the repository service provider of their obligations if applicable.

2.1.4 RA Obligations

An RA who performs registration functions as described in this policy shall comply with the stipulations of this policy, and comply with a CPS approved by the PA for use with this policy. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities. An RA supporting this policy shall conform to the stipulations of this document, including—

- Maintaining its operations in conformance to the stipulations of the approved CPS.
- Including only valid and appropriate information in certificate requests, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate.
- Ensuring that obligations are imposed on subscribers in accordance with Section 2.1.3, and that subscribers are informed of the consequences of not complying with those obligations.

2.1.5 Subscriber Obligations

Subscribers shall—

- Accurately represent themselves in all communications with the PKI authorities and other subscribers.
- Protect their private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements and local procedures.
- Notify, in a timely manner, the CA that issued their certificates of suspicion that their private keys are compromised or lost. Such notification shall be made directly, or indirectly through mechanisms consistent with the CA's CPS.
- Abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates.

2.1.6 Relying Party Obligations

This CP does not specify the steps a relying party should take to determine whether to rely upon a certificate. The relying party decides, pursuant to its own policies, what steps to take. The CA merely provides the tools (i.e., certificates and CRLs) needed to perform the trust path creation, validation, and CP mappings that the relying party may wish to employ in its determination.

2.1.7 Repository Obligations

All CAs that issue certificates under this policy are obligated to post all CA certificates and all CRLs in a directory that is publicly accessible through the Lightweight Directory Access Protocol. CAs may optionally post subscriber certificates in this directory in accordance with agency policy. To promote consistent access to certificates and CRLs, the repository shall implement access controls to prevent modification or deletion of information.

Posted certificates and CRLs may be replicated in additional repositories for performance enhancement. Such repositories may be operated by the CA or other parties (e.g., Federal agencies).

2.2 LIABILITY

The U.S. Government shall not be liable to any party, except as determined pursuant to the Federal Tort Claims Act (FTCA), 28 U.S.C. 2671-2680, or as determined through a valid express written contract between the Government and another party.

2.3 FINANCIAL RESPONSIBILITY

This CP contains no limits on the use of certificates issued by CAs under this policy. Rather, entities, acting as Relying Parties, shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction.

2.3.1 Indemnification by Relying Parties and Subscribers

No stipulation.

2.3.2 Fiduciary Relationships

No stipulation.

2.4 INTERPRETATION AND ENFORCEMENT

The terms and provisions of this Certificate Policy shall be interpreted under and governed by applicable Federal law.

2.4.1 Severability of Provisions, Survival, Merger, and Notice

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in Section 8.1

2.4.2 Dispute Resolution Procedures

The PA shall facilitate the resolution between entities when conflicts arise as a result of the use of certificates issued under this policy. When the dispute is between Federal agencies, and the PA is unable to facilitate resolution, dispute resolution may be escalated to OMB or U.S. Department of Justice, Office of Legal Counsel as necessary.

2.5 FEES

No stipulation.

2.6 PUBLICATION AND REPOSITORY

2.6.1 Publication of CA Information

Certificates and CRLs shall be published as specified in Section 2.1.6. No stipulation regarding publication of additional CA information.

2.6.2 Frequency of Publication

Certificates are published following subscriber acceptance as specified in Section 4.3 and proof of possession of private key as specified in Section 3.1.7. The CRL is published as specified in Section 4.4.3.1. All information to be published in the repository shall be published promptly after such information becomes available to the CA. The CA shall specify in its CPS time limits within which it will publish various types of information.

2.6.3 Access Controls

The CA shall protect information not intended for public dissemination or modification. CA certificates and CRLs in the repository shall be publicly available through the Internet. Access to other information in the CA repositories shall be determined by agencies pursuant to their authorizing and controlling statutes. The CPS shall detail what information in the repository shall be exempt from automatic availability and to whom, and under which conditions, the restricted information may be made available.

2.6.4 Repositories

See Section 2.1.5.

2.7 COMPLIANCE AUDIT

2.7.1 Frequency of Entity Compliance Audit

CAs and RAs operating under this policy shall conduct a compliance audit no less than once every year. Additionally, the PA has the right to require aperiodic inspections of CAs and RAs to validate that the CA/RA is operating in accordance with their CPS.

2.7.2 Identity/Qualifications of Compliance Auditor

The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the CA's CPS and this CP.

2.7.3 Compliance Auditor's Relationship to Audited Party

The compliance auditor either shall be a private firm, which is independent from the entities (CA and RAs) being audited, or it shall be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation. An example of the latter situation may be an Agency inspector general. The PA shall determine whether a compliance auditor meets this requirement.

The Agency PMA is responsible for identifying and engaging a qualified auditor of agency operations implementing aspects of this CP.

2.7.4 Topics Covered by Compliance Audit

The purpose of a compliance audit shall be to verify that a CA and its recognized RAs comply with all the requirements of the current versions of this CP and the CA’s CPS. All aspects of the CA/RA operation shall be subject to compliance audit inspections.

2.7.5 Actions taken as a result of deficiency

When the compliance auditor finds a discrepancy between the requirements of this CP or the stipulations in the CPS and the design, operation, or maintenance of the PKI Authorities, the following actions shall be performed:

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall notify the parties identified in Section 2.7.6 of the discrepancy;
- The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to the PA and appropriate Agency PMA.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the PA may decide to temporarily halt operation of the CA or RA, to revoke a certificate issued to the CA or RA, or take other actions it deems appropriate. The PA will develop procedures for making and implementing such determinations.

2.7.6 Communication of Results

An Audit Compliance Report shall be provided to the CA. After 30 days, the Audit Compliance Report and identification of corrective measures taken or being taken by the CA or RA shall be provided to both the PA and (where applicable) the Agency PMA. A special compliance audit may be required to confirm the implementation and effectiveness of the remedy.

2.8 CONFIDENTIALITY

CA information not requiring protection shall be made publicly available. Public access to organizational information shall be determined by the respective organization.

2.9 INTELLECTUAL PROPERTY RIGHTS

No stipulation.

3. IDENTIFICATION AND AUTHENTICATION

3.1 INITIAL REGISTRATION

3.1.1 Types of Names

For certificates issued under id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-High, and id-fpki-common-devices, the CA shall assign X.500 distinguished names to all subscribers. These distinguished names may be in either of two forms: an X.501 distinguished name specifying a geo-political name; or an Internet domain component name.

All geo-political X.501 distinguished names assigned to federal employees shall be in one of the following directory information trees:

C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*]
C=US, [o=*department*], [ou=*agency*], [ou=*structural_container*]

New implementations shall assign names in the following directory tree:
C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*]

The organizational units *department* and *agency* appear when applicable and are used to specify the federal entity that employs the subscriber. At least one organizational unit must appear in the DN. The additional organizational unit *structural_container* is permitted to support local directory requirements, such as differentiation between human subscribers and devices. This organizational unit may not be employed to further differentiate between subcomponents within an agency.

The distinguished name of the federal employee subscriber will take one of the three following forms:

- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], cn=*nickname lastname*
- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], cn=*firstname initial. lastname*
- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], cn=*firstname middlename lastname*

In the first name form, *nickname* may be the subscriber's first name, a form of the first name, middle name, or pseudonym (e.g., Buck) by which the subscriber is generally known. A generational qualifier, such as "Sr." or "III", may be appended to any of the common name forms specified above.

X.501 distinguished names assigned to federal contractors and other affiliated persons shall be within the same directory information tree. The distinguished name of the federal contractor subscribers and affiliate subscribers will take one of the three following forms:

- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], cn=*nickname lastname* (affiliate)
- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], cn=*firstname initial. lastname* (affiliate)
- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], cn=*firstname middlename lastname* (affiliate)

For names assigned to federal contractors and other affiliated persons, generational qualifiers may be inserted between *lastname* and "(affiliate)".

Legacy implementations which predate this policy may use the directory tree:
C=US, [o=*department*], [ou=*agency*], [ou=*structural_container*]
Common name fields shall be populated as specified above.

Distinguished names based on Internet domain component names shall be in the following directory information trees:

dc=gov, dc=*org0*, [dc=*org1*],…[dc=*orgN*], [ou=*structural_container*]
dc=mil, dc=*org0*, [dc=*org1*],…[dc=*orgN*], [ou=*structural_container*]

The default Internet domain name for the agency, [*orgN*.]…[*org0*].gov or [*orgN*.]…[*org0*].mil will be used to determine DNs. The first domain component of the DN will either be dc=gov or dc=mil. At least, the *org0* domain component must appear in the DN. The *org1* to *orgN* domain components appear, in order, when applicable and are used to specify the federal entity that employs the subscriber.

The distinguished name of the federal employee subscriber may take one of the three following forms when their agency's Internet domain name ends in .gov:

- dc=gov, dc=*org0*, [dc=*org1*], …[dc=*orgN*], [ou=*structural_container*], cn=*nickname lastname*
- dc=gov, dc=*org0*, [dc=*org1*],…[dc=*orgN*], [ou=*structural_container*], cn=*firstname initial. lastname*
- dc=gov, dc=*org0*, [dc=*org1*],…[dc=*orgN*], [ou=*structural_container*], cn=*firstname middlename lastname*

The distinguished name of the federal contractors and affiliated subscribers may take one of the three following forms when the agency's Internet domain name ends in .gov:

- dc=gov, dc=*org0*, [dc=*org1*],…[dc=*orgN*], [ou=*structural_container*], cn=*nickname lastname* (affiliate)
- dc=gov, dc=*org0*, [dc=*org1*],…[dc=*orgN*], [ou=*structural_container*], cn=*firstname initial. lastname* (affiliate)
- dc=gov, dc=*org0*, [dc=*org1*],…[dc=*orgN*], [ou=*structural_container*], cn=*firstname middlename lastname* (affiliate)

The distinguished name of the federal employee subscriber may take one of the three following forms when their agency's Internet domain name ends in .mil:

- dc=mil, dc=*org0*, [dc=*org1*], …[dc=*orgN*], [ou=*structural_container*], cn=*nickname lastname*
- dc=mil, dc=*org0*, [dc=*org1*],…[dc=*orgN*], [ou=*structural_container*], cn=*firstname initial. lastname*
- dc=mil, dc=*org0*, [dc=*org1*],…[dc=*orgN*], [ou=*structural_container*], cn=*firstname middlename lastname*

The distinguished name of the federal contractors and affiliated subscribers may take one of the three following forms when the agency's Internet domain name ends in .mil:

- dc=mil, dc=*org0*, [dc=*org1*],…[dc=*orgN*], [ou=*structural_container*], cn=*nickname lastname* (affiliate)
- dc=mil, dc=*org0*, [dc=*org1*],…[dc=*orgN*], [ou=*structural_container*], cn=*firstname initial. lastname* (affiliate)
- dc=mil, dc=*org0*, [dc=*org1*],…[dc=*orgN*], [ou=*structural_container*], cn=*firstname middlename lastname* (affiliate)

The CA may supplement any of the name forms for users specified in this section by including a dnQualifier, serial number, or user id attribute. When any of these attributes are included, they may appear as part of a multi-valued RDN with the common name or as a distinct attribute. Generational qualifiers may optionally be included in common name attributes in distinguished names based on Internet domain names. For names assigned to employees, generational qualifiers may be appended to the common name. For names assigned to federal contractors and other affiliated persons, generational qualifiers may be inserted between *lastname* and "(affiliate)".

Devices that are the subject of certificates issued under this policy may be assigned either a geo-political name or an Internet domain component name. Device names may take the following forms:

- C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=*structural_container*], cn=*device name*
- dc=gov, dc=*org0*, [*dc=org1*], …[dc=*orgN*], [ou=*structural_container*], [cn=*device name*]
- dc=mil, dc=*org0*, [*dc=org1*], …[dc=*orgN*], [ou=*structural_container*], [cn=*device name*]

where *device name* is a descriptive name for the device. Where a device is fully described by the Internet domain name, the common name attribute is optional.

This policy does not restrict the directory information tree for names of CAs. However, CAs that issue certificates under this policy must have distinguished names. CA distinguished names may be either a geo-political name or an Internet domain component name.

CA geo-political distinguished names may be composed of any combination of the following attributes: country; organization; organizational unit; and common name. Internet domain component names are composed of the following attributes: domain component; organizational unit; and common name.

For certificates issued under id-fpki-common-authentication, assignment of X.500 distinguished names is optional. If assigned, distinguished names shall follow the rules specified above for id-fpki-common-hardware. Certificates issued under id-fpki-common-authentication shall include a subject alternative name. At a minimum, the subject alternative name extension shall include the pivFASC-N name type [FIPS 201]. The value for this name shall be the FASC-N [PACS] of the subject's PIV card.

Certificates issued under id-fpki-common-cardAuth shall include a subject alternative name extension that includes the pivFASC-N name type. The value for this name shall be the FASC-N of the subject's PIV card. Certificates issued under id-fpki-common-cardAuth shall not include any other name in the subject alternative name extension but may include a non-NULL name in the subject field. If included, the subject distinguished name shall take the following form:

- C=US, o=U.S. Government, [ou=*department*], [ou=*agency*], [ou=*structural_container*], serialNumber=*FASC-N*

Practice Note: The FASC-N [PACS] consists of 40 decimal digits that are encoded as a 25-byte binary value. This 25-byte binary value may be encoded directly into the pivFASC-N name type in the subject alternative name extension, but when included in the subject field the FASC-N must be encoded as a PrintableString that is at most 64 characters long. This policy does not mandate any particular method for encoding the FASC-N within the serial number attribute as long as the same encoding method is used for all certificates issued by a CA. Acceptable methods for encoding the FASC-N within the serial number attribute include encoding the 25-byte binary value as 50 bytes of ASCII HEX or encoding the 40 decimal digits as 40 bytes of ASCII decimal.

3.1.2 Need for Names to be Meaningful

The subscriber certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates can be understood and used by relying parties. Names used in the certificates must identify in a meaningful way the subscriber to which they are assigned.

The common name in the DN must represent the subscriber in a way that is easily understandable for humans. For people, this will typically be a legal name, so the preferred common name form is

cn=*firstname initial. lastname*

While the issuer name in CA certificates is not generally interpreted by relying parties, this CP still requires use of meaningful names by CAs issuing under this policy. If included, the common name should describe the issuer, such as:

cn=*AgencyX CA-3*.

The subject name in CA certificates must match the issuer name in certificates issued by the subject, as required by RFC 3280, even if the subject's name is not meaningful.

3.1.3 Rules for Interpreting Various Name Forms

Rules for interpreting distinguished name forms are specified in [USGold]. Rules for interpreting the pivFASC-N name type are specified in [PACS].

3.1.4 Uniqueness of Names

Name uniqueness for certificates issued by each CA must be enforced. Each CA and its associated RAs shall enforce name uniqueness within the X.500 name space. When other name forms are used, they too must be allocated such that name uniqueness is ensured for certificates issued by that CA.

The CPS shall identify one or more directory information trees for the assignment of subject names. Directory information trees may be assigned to a single CA, or shared between CAs. Where multiple CAs share a single directory information tree, the PA shall review and approve procedures for name space control.

3.1.5 Name Claim Dispute Resolution Procedure

The PA shall resolve any name collisions brought to its attention. Agency PMAs shall resolve name collisions within their own name space.

3.1.6 Recognition, Authentication and Role of Trademarks

No stipulation.

3.1.7 Method to Prove Possession of Private Key

In all cases where the party named in a certificate generates its own keys that party shall be required to prove possession of the private key, which corresponds to the public key in the certificate request. For signature keys, this may be done by the entity using its private key to sign a value supplied by the CA. The CA shall then validate the signature using the party's public key. The PA may allow other mechanisms that are at least as secure as those cited here.

In the case where key generation is performed under the CA or RA's direct control, proof of possession is not required.

3.1.8 Authentication for CA Certificate Issuance

Requests for CA certificates shall include the CA name, address, and documentation of the existence of the CA. The issuing CA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the CA.

3.1.9 Authentication of Individual Identity

Procedures used by agencies to issue identification to their own personnel and affiliates may be more stringent than that set forth below. When this is the case, the agency procedures for authentication of personnel shall apply in addition to the guidance in this section.

The RA shall ensure that the applicant's identity information is verified. RAs may accept notarized authentication of an applicant's identity to support identity proofing of remote applicants, assuming agency identity badging requirements are otherwise satisfied. Minimal procedures for RA authentication and notarized authentication of employees and affiliated personnel are detailed below.

At a minimum, authentication procedures for employees must include the following steps:

1) Verify that a request for certificate issuance to the applicant was submitted by agency management;

2) Applicant's employment shall be verified through use of official agency records.

3) Applicant's identity shall be established by in-person proofing before the Registration Authority, based on either of the following processes:

    a) Process #1:

        i) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and

        ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g. a photograph on the credential itself or a securely linked photograph of applicant), and

        iii) The credential presented in step 3) a) i) above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). Typically this is accomplished by querying a database maintained by the organization that issued the credential, but other equivalent methods may be used.

    b) Process #2:

        i) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and

        ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a photograph of applicant securely stored and linked to the credential), and

iii) The applicant presents current corroborating information (e.g., current credit card bill or recent utility bill) to the RA. The RA verifies the identifying information (e.g., name and address) on the credential presented in step 3) b) i) above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). [Practice Note: This may be accomplished by querying a database maintained by the organization that issued the financial instrument or through use of a commercial credit database. In some instances, commercial credit card databases will validate name and address of current cardholders online; this validation is acceptable if the card is presented to the RA. Other methods may be accepted.]

4) A biometric of the applicant (e.g., a photograph or fingerprint) shall be recorded and maintained by the RA or CA. (Handwritten signatures and other behavioral characteristics are not accepted as biometrics for the purposes of this policy.) This establishes an audit trail for dispute resolution.

For contractors and other affiliated personnel, the authentication procedures must include the following steps:

1) Verify that a request for certificate issuance to the applicant was submitted by an authorized sponsoring agency employee (e.g., contracting officer or contracting officer's technical representative);

2) Sponsoring Agency employee's identity and employment shall be verified through either of the following methods:

   a) A digital signature verified by a currently valid employee signature certificate issued by the CA, may be accepted as proof of both employment and identity, or

   b) Employee's identity shall be established by in-person proofing before the Registration Authority as in employee authentication above and employment validated through use of the official agency records.

3) Applicant's identity shall be established by in-person proofing before the Registration Authority, based on either of the following processes:

   a) Process #1:

      i) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and

      ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g. a photograph on the credential itself or a securely linked photograph of applicant), and

      iii) The credential presented in step 3) a) i) above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). Typically this is accomplished by querying official records maintained by the organization that issued the credential.

   b) Process #2:

i) The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and

ii) The RA examines the presented credential for biometric data that can be linked to the applicant (e.g. a photograph on the credential itself or a securely linked photograph of applicant), and

iii) The applicant presents current corroborating information (e.g., current credit card bill or recent utility bill) to the RA. The RA verifies the information (e.g., name and address) on the credential presented in step 3) b) i) above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). Typically this is accomplished by querying a database maintained by the organization that issued the financial instrument or through use of a commercial credit database. In some instances, commercial credit card databases will validate name and address of current cardholders online; this validation is acceptable if the card is presented to the RA.

4) A biometric of the applicant (e.g., a photograph or fingerprint) shall be recorded and maintained by the RA or CA.

Additionally, the RA shall record the process that was followed for issuance of each certificate. The process documentation and authentication requirements shall include the following:

- The identity of the person performing the identification;
- A signed declaration by that person that he or she verified the identity of the Applicant as required by the CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury);
- Unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- The biometric of the applicant;
- The date and time of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury).

Where it is not possible for applicants to appear in person before the RA, a trusted agent may serve as proxy for the RA. The trusted agent forwards the information collected from the applicant directly to the RA in a secure manner. The requirement for recording a biometric of the applicant may be satisfied by providing passport-style photographs to the notary. The trusted agent shall verify the photographs against the appearance of the applicant and the biometrics on the presented credentials and securely incorporate the biometric as a component in the notarized package. Packages secured in a tamper-evident manner by the trusted agent satisfy this requirement; other secure methods are also acceptable.

Authentication by a trusted agent does not relieve the RA of its responsibility to perform steps 1), 2), the verification of identifying information (e.g., by checking official records) in step 3), and the maintenance of biometrics in step 4), above.

3.1.10 Authentication of Component Identities

Some computing and communications devices (routers, firewalls, servers, etc.) will be named as certificate subjects. In such cases, the device must have a human sponsor. The sponsor is responsible for providing the following registration information:

- Equipment identification (e.g., serial number) or service name (e.g., DNS name)
- Equipment public keys
- Equipment authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the sponsor when required

The identity of the sponsor shall be authenticated by:

- Verification of digitally signed messages sent from the sponsor using a certificate issued under this policy; or
- In person registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of **Section 3.1.9**.

3.2 CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY

The procedures for accomplishing the Certificate Renewal, Update, and Routine Re-Key specified in this CP will be detailed in the CA's CPS.

3.2.1 Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but with a new, extended validity period and a new serial number. Subscriber certificates issued under this policy shall not be renewed, except during recovery from CA key compromise (see 4.8.3). CA certificates and OCSP responder certificates may be renewed.

3.2.2 Certificate Re-Key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a subscriber periodically obtain new keys. (Section 6.3.2 establishes usage periods for private keys for both CAs and subscribers.) Re-keying a certificate means that a new certificate is created that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key) and a different serial number, and it may be assigned a different validity period.

For policies other than id-fpki-common-High, if it has been less than 6 years since a subscriber was identified as required in Section 3.1, a CA may authenticate an electronic request for a new certificate using the currently valid certificate issued to the subscriber by the CA. Subscribers shall identify themselves for the purpose of re-keying through use of current signature key.

If more than 6 years have passed since a subscriber's identity was authenticated as specified in Section 3.1, a subscriber certificate re-key shall follow the same procedures as initial certificate issuance.

CA certificate Re-Key and re-key of certificates issued under id-fpki-common-High shall follow the same procedures as initial certificate issuance.

3.2.3 Certificate Update

Updating a certificate means creating a new certificate that has the same or a different key and a different serial number, and that differs in one or more other fields from the old certificate. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or updated.

If an individual's name changes (e.g., due to marriage), then proof of the name change must be provided to the RA or other designated agent in order for a certificate with the new name to be issued. If an individual's authorizations or privileges change, the RA will verify those authorizations. If authorizations have reduced, the old certificate must be revoked.

Finally, when a CA updates its private signature key and thus generates a new public key, the CA shall notify all CAs, RAs, and subscribers that rely on the CA's certificate that it has been changed. CAs that distribute self-signed certificates shall generate key rollover certificates, where the new public key is signed by the old private key, and vice versa. This permits acceptance of newly issued certificates and CRLs without distribution of the new self-signed certificate to current users. Key rollover certificates are optional for CAs that do not distribute self-signed certificates.

Where distribution of the new self-signed certificate to current users is required, such certificates shall be conveyed to users in a secure fashion to preclude malicious substitution attacks.

3.3 OBTAINING A NEW CERTIFICATE AFTER REVOCATION

In the event of certificate revocation, issuance of a new certificate shall always require that the party go through the initial registration process per Section 3.1 above.

3.4 REVOCATION REQUEST

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised.

4. OPERATIONAL REQUIREMENTS

4.1 APPLICATION FOR A CERTIFICATE

The PKI Authorities must perform the following steps when an applicant (prospective subscriber) applies for a certificate:

- Establish the applicant's authorization (by the employing or sponsoring agency) to obtain a certificate. (per Section 3.1)
- Establish and record identity of the applicant (per Section 3.1)
- Obtain the applicant's public key and verify the applicant's possession of the private key for each certificate required (per Section 3.1.7)
- Verify any role or authorization information requested for inclusion in the certificate.

These steps may be performed in any order that is convenient for the PKI Authorities and applicants and does not defeat security, but all must be completed before certificate issuance. All communications among PKI Authorities supporting the certificate application and issuance process shall be authenticated and protected from modification; any electronic transmission of shared secrets shall be protected. Communications may be electronic or out-of-band. Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair shall be used. Out-of-band communications shall protect the confidentiality and integrity of the data.

4.1.1 Delivery of Public Key for Certificate Issuance

Public keys must be delivered for certificate issuance in a way that binds the applicant principal's verified identification to the public key. This binding may be accomplished using cryptography. If cryptography is used it must be at least as strong as that employed at certificate issuance. This binding may be accomplished using non-cryptographic physical and procedural mechanisms. Regardless of the method selected, the mechanism used for public key delivery shall be set forth in the CA's CPS.

In those cases where public/private key pairs are generated by the CA on behalf of the subscriber, the CA shall implement secure mechanisms to ensure that the token on which the public/private key pair is held is securely sent to the proper subscriber. The CA shall also implement procedures to ensure that the token is not activated by an unauthorized entity.

4.2 CERTIFICATE ISSUANCE

Upon receiving the request, the CAs/RAs will—

- Verify the identity of the requestor
- Verify the authority of the requestor and the integrity of the information in the certificate request
- Build and sign a certificate if all certificate requirements have been met (in the case of an RA, have the CA sign the certificate)
- Make the certificate available to the subscriber.

The certificate request may already contain a certificate built by either the RA or the subscriber. This certificate will not be signed until all verifications and modifications, if any, have been completed to the CA's satisfaction.

All authorization and other attribute information received from a prospective subscriber shall be verified before inclusion in a certificate. The responsibility for verifying prospective subscriber data shall be described in a CA's CPS.

4.2.1 Delivery of Subscriber's Private Key to Subscriber

A private key will be generated within the boundary of a cryptographic module, as described in 6.2.6. If the owner of the cryptographic token generates the key, there is no need to deliver the private key. If the key is generated elsewhere, the cryptographic token must be delivered to the subscriber. Accountability for the location and state of the cryptographic token must be maintained until the subscriber accepts possession of it. The subscriber shall acknowledge receipt of the cryptographic token. Anyone who generates a private signing key for a subscriber shall not retain any copy of the key. Cryptographic tokens containing CA private signature keys may be backed up in accordance with security audit requirements defined Section 4.5.

This policy allows a certificate to be issued only to a single subscriber. Certificates shall not be issued that contain a public key whose associated private key is shared. [Practice Note: CAs that issue certificates under this policy may simultaneously operate under a policy that permits issuance of certificates whose associated private key is shared. Such certificates *must* assert a different policy OID.]

4.2.2 Public Key Delivery and Use

The public key of the CA must be available for certification trust paths to be created and verified. In general, CA certificates are published in the public repository (see 2.1.5) operated by the PA, and the verification of public keys is performed using X.509 path validation.

Where users rely on the CA's public key as a trust anchor, publication in the repository does not permit verification of the public key. To extract the key from a certificate with confidence that it has not been altered, the CA must ensure that its users have obtained a self-signed CA certificate through trusted procedural mechanisms. Such a self-signed CA certificate is sometimes called a Self-signed Root Certificate, or Trusted Certificate. This document will use the term Trusted Certificate.

Acceptable methods for Trusted Certificate delivery include but are not limited to—

- The RA loading a Trusted Certificate onto tokens delivered to relying parties via secure mechanisms, such as:
    - The Trusted Certificate is loaded onto the token during the subscriber's appearance at the RA.
    - The Trusted Certificate is loaded onto the token when the RA generates the subscriber's key pair and loads the private key onto the token.
- Distribution of Trusted Certificates through secure out-of-band mechanisms;
- Comparison of certificate hashes or fingerprints against Trusted Certificate hashes or fingerprints made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the certificate are not acceptable as an authentication mechanism); or
- Loading certificates from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded.

CAs that distribute Trusted Certificates will create key rollover certificates as a consequence of CA re-key. The new CA keys may be used securely (through the X.509 path validation algorithm) without explicit delivery of the public key to subscribers.

4.3 CERTIFICATE ACCEPTANCE

Before a subscriber can make effective use of its private key, a PKI Authority shall—

- Explain to the subscriber its responsibilities as defined in Section 2.1.5
- Inform the subscriber of the creation of a certificate and the contents of the certificate.

The ordering of this process, and the mechanisms used, will depend on factors such as where the key is generated and how certificates are posted.

4.4 CERTIFICATE SUSPENSION AND REVOCATION

4.4.1 Revocation

4.4.1.1 Circumstances for Revocation

A certificate shall be revoked when the binding between the subject and the subject's public key defined within a certificate is no longer considered valid. Examples of circumstances that invalidate the binding are—

- Identifying information or affiliation components of any names in the certificate becomes invalid.
- Privilege attributes asserted in the subscriber's certificate are reduced.
- The subscriber can be shown to have violated the stipulations of its subscriber agreement.
- There is reason to believe the private key has been compromised.
- The subscriber or other authorized party (as defined in the CPS) asks for his/her certificate to be revoked.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

4.4.1.2 Who Can Request a Revocation

Within the PKI, a CA may summarily revoke certificates within its domain. A written notice and brief explanation for the revocation shall subsequently be provided to the subscriber. The RA can request the revocation of a subscriber's certificate on behalf of any authorized party as specified in the CPS. A subscriber may request that it's own certificate be revoked. Other authorized agency officials may request revocation as described in the CPS.

4.4.1.3 Procedure for Revocation Request

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). The steps involved in the process of requesting a certification revocation are detailed in the CPS.

4.4.1.4 Revocation Request Grace Period

There is no grace period for revocation under this policy; CAs will revoke certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests shall be processed before the next CRL is published, excepting those requests received within two hours of CRL issuance. Revocation requests received within two hours of CRL issuance shall be processed before the following CRL is published.

4.4.2 Suspension

Certificate suspension for CA certificates is not allowed by this policy. However, the use of certificate suspension for end entity certificates is allowed.

4.4.3 CRLs

CAs shall issue CRLs covering all unexpired certificates issued under this policy except for OCSP Responder certificates that include the id-pkix-ocsp-nocheck extension.

4.4.3.1 CRL Issuance Frequency

CRLs shall be issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below.

Certificate status information shall be published not later than the next scheduled update. This will facilitate the local caching of certificate status information for offline or remote (laptop) operation.

CAs shall make public a description of how to obtain revocation information for the certificates they publish, and an explanation of the consequences of using dated revocation information. This information shall be given to subscribers during certificate request or issuance, and shall be readily available to any potential relying party.

CAs that only issue certificates to CAs and that operate offline must issue CRLs at least once every 24 hours, and the *nextUpdate* time in the CRL may be no later than 24 hours after issuance time (i.e. the *thisUpdate* time). CAs that issue certificates to subscribers or operate online must issue CRLs at least once every 18 hours, and the *nextUpdate* time in the CRL may be no later than 18 hours after issuance time (i.e. the *thisUpdate* time). When a CA certificate or subscriber certificate issued under id-fpki-common-High is revoked because of compromise, or suspected compromise, of a private key, a CRL must be issued within 6 hours of notification.

4.4.4 Online Revocation/Status Checking Availability

CAs shall support online status checking via OCSP [RFC 2560] for end entity certificates issued under id-fpki-common-authentication and id-fpki-common-cardAuth. Status information maintained by the OCSP server must be updated regularly. Where a certificate is revoked for key compromise, the status information must be updated and available to relying parties within 6 hours. Where a certificate is revoked for a reason other than key compromise, the status information must be updated and available to relying parties within 18 hours. CAs that do not issue certificates under id-fpki-common-authentication and relying party client software may optionally support online status checking. Because not all operational environments can accommodate online communications, all CAs will be required to support CRLs. Client software using online status checking need not obtain or process CRLs.

4.4.5 Other Forms of Revocation Advertisements Available

A CA may also use other methods to publicize the certificates it has revoked. Any alternative method must meet the following requirements:

- The alternative method must be described in the CA's approved CPS;

- The alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified.

4.4.6 Checking Requirements for Other Forms of Revocation Advertisements

No stipulation.

4.4.7 Special Requirements Related to Key Compromise

In the event of a CA private key compromise, the following operations must be performed.

If the CA distributed the private key in a Trusted Certificate, the CA shall perform the following operations:

- Generate a new signing key pair and corresponding Trusted Certificate;
- Initiate procedures to notify subscribers of the compromise; and
- Securely distribute the Trusted Certificate.
- Optionally, the CA may renew current certificates under the new signing key. (see 3.2.1)

If the CA's private key appears as the subject public key in certificates issued by other CAs, the CA will notify the issuer(s) of these certificates within 24 hours.

4.5 SECURITY AUDIT PROCEDURE

Audit log files shall be generated for all events relating to the security of the CA. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with Section 4.5.3, *Retention Period for Security Audit Data*.

4.5.1 Types of Events Recorded

All security auditing capabilities of CA operating system and PKI CA applications shall be enabled during installation. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event
- The date and time the event occurred
- A success or failure indicator when executing the CA's signing process
- A success or failure indicator when performing certificate revocation
- The identity of the entity and/or operator that caused the event.

A message from any source requesting an action by the CA is an auditable event; the message must include message date and time, source, destination, and contents.

The CA shall record the events identified in the list below. Where these events cannot be electronically logged, the CA shall supplement electronic audit logs with physical logs as necessary.

- SECURITY AUDIT:
  - Any changes to the Audit parameters, e.g., audit frequency, type of event audited
  - Any attempt to delete or modify the Audit logs
  - Obtaining a third-party time-stamp
- IDENTIFICATION AND AUTHENTICATION:
  - Successful and unsuccessful attempts to assume a role
  - The value of maximum authentication attempts is changed
  - Maximum authentication attempts unsuccessful authentication attempts occur during user login
  - An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
  - An Administrator changes the type of authenticator, e.g., from password to biometrics
- LOCAL DATA ENTRY:
  - All security-relevant data that is entered in the system
- REMOTE DATA ENTRY:
  - All security-relevant messages that are received by the system
- DATA EXPORT AND OUTPUT:
  - All successful and unsuccessful requests for confidential and security-relevant information
- KEY GENERATION:
  - Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)
- PRIVATE KEY LOAD AND STORAGE:
  - The loading of Component private keys
  - All access to certificate subject private keys retained within the CA for key recovery purposes
- TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE:
  - All changes to the trusted public keys, including additions and deletions
- SECRET KEY STORAGE:
  - The manual entry of secret keys used for authentication
- PRIVATE AND SECRET KEY EXPORT:
  - The export of private and secret keys (keys used for a single session or message are excluded)
- CERTIFICATE REGISTRATION:
  - All certificate requests
- CERTIFICATE REVOCATION:
  - All certificate revocation requests

- CERTIFICATE STATUS CHANGE APPROVAL:
    - The approval or rejection of a certificate status change request
- CA CONFIGURATION:
    - Any security-relevant changes to the configuration of the CA
- ACCOUNT ADMINISTRATION:
    - Roles and users are added or deleted
    - The access control privileges of a user account or a role are modified
- CERTIFICATE PROFILE MANAGEMENT
    - All changes to the certificate profile
- REVOCATION PROFILE MANAGEMENT
    - All changes to the revocation profile
- CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT
    - All changes to the certificate revocation list profile
- MISCELLANEOUS
    - Appointment of an individual to a Trusted Role
    - Designation of personnel for multiparty control
    - Installation of the Operating System
    - Installation of the FBCA or Entity CA
    - Installing hardware cryptographic modules
    - Removing hardware cryptographic modules
    - Destruction of cryptographic modules
    - System Startup
    - Logon Attempts to FBCA or Entity CA Apps
    - Receipt of Hardware / Software
    - Attempts to set passwords
    - Attempts to modify passwords
    - Backing up FBCA or Entity CA internal database
    - Restoring FBCA or Entity CA internal database
    - File manipulation (e.g., creation, renaming, moving)
    - Posting of any material to a repository
    - Access to FBCA or Entity CA internal database
    - All certificate compromise notification requests
    - Loading tokens with certificates
    - Shipment of Tokens
    - Zeroizing tokens
    - Rekey of the FBCA or Entity CA
    - Configuration changes to the CA server involving:
        - Hardware
        - Software
        - Operating System
        - Patches

        - Security Profiles
- PHYSICAL ACCESS / SITE SECURITY
    - Personnel Access to room housing FBCA or Entity CA
    - Access to the FBCA or Entity CA server
    - Known or suspected violations of physical security
- ANOMALIES
    - Software Error conditions
    - Software check integrity failures
    - Receipt of improper messages
    - Misrouted messages
    - Network attacks (suspected or confirmed)
    - Equipment failure
    - Electrical power outages
    - Uninterruptible Power Supply (UPS) failure
    - Obvious and significant network service or access failures
    - Violations of Certificate Policy
    - Violations of Certification Practice Statement
    - Resetting Operating System clock

4.5.2 Frequency of Processing Data

For CAs that issue certificates under id-fpki-common-High, review of the audit log shall be required at least once every month. For CAs that do not issue certificates under id-fpki-common-High, review of the audit log shall be required at least once every two months.

Such reviews involve verifying that the log has not been tampered with and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. A statistically significant portion of the security audit data generated by the CA since the last review shall be examined. This amount will be described in the CPS.

All significant events shall be explained in an audit log summary. Actions taken as a result of these reviews shall be documented.

4.5.3 Retention Period for Security Audit Data

Audit logs shall be retained onsite for at least 2 months in addition to being retained in the manner described below. The individual who removes audit logs from the CA system shall be an official different from the individuals who, in combination, command the CA signature key.

4.5.4 Protection of Security Audit Data

The security audit data shall not be open for reading or modification by any human, or by any automated process, other than those that perform security audit processing. CA system configuration and procedures must be implemented together to ensure that only authorized people archive or delete security audit data. Procedures must be implemented to protect archived data from deletion or destruction before the end of the security audit data retention period (note that deletion requires modification access). Security audit data shall be moved to a safe, secure storage location separate from the CA equipment.

4.5.5 Security Audit Data Backup Procedures

Audit logs and audit summaries shall be backed up at least monthly. A copy of the audit log shall be sent offsite in accordance with the CPS, on a monthly basis.

4.5.6 Security Audit Collection System (Internal vs. External)

The audit log collection system may or may not be external to the CA system. Automated audit processes shall be invoked at system or application startup, and cease only at system or application shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, operations shall be suspended until the problem has been remedied. The PA shall determine whether to resume operations.

4.5.7 Notification to Event-Causing Subject

There is no requirement to notify a subject that an event was audited. Real-time alerts are neither required nor prohibited by this policy.

4.5.8 Vulnerability Assessments

The CA will perform routine self-assessments of security controls.

4.6 RECORDS ARCHIVAL

4.6.1 Types of Events Archived

CA archive records shall be sufficiently detailed to determine the proper operation of the CA and the validity of any certificate (including those revoked or expired) issued by the CA. At a minimum, the following data shall be recorded for archive:

- CA accreditation (if applicable)
- Certificate Policy
- Certification Practice Statement
- Contractual obligations
- Other agreements concerning operations of the CA
- System and equipment configuration
- Modifications and updates to system or configuration
- Certificate requests
- All certificates issued and/or published
- Record of Re-key
- Security audit data (in accordance with Section 4.5)
- Revocation requests
- Subscriber identity Authentication data as per Section 3.1.9
- Subscriber agreements
- Documentation of receipt of tokens
- All CARLs and CRLs issued and/or published
- Other data or applications to verify archive contents

- Documentation required by compliance auditors

In addition, CAs that retain subscriber private encryption keys for business continuity purposes shall archive such subscriber private keys.

4.6.2 Retention Period for Archive

For CAs that issue certificates under id-fpki-common-High, archive records must be kept for a minimum of 20 years and 6 months without any loss of data.

For CAs that do not issue certificates under id-fpki-common-High, archive records must be kept for a minimum of 10 years and 6 months without any loss of data.

4.6.3 Protection of Archive

No unauthorized user shall be permitted to write to, modify, or delete the archive. For the CA, archived records may be moved to another medium. The contents of the archive shall not be released except (1) in accordance with agency policy, or (2) as required by law. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. Archive media shall be stored in a safe, secure storage facility separate from the CA.

4.6.4 Archive Backup Procedures

No stipulation.

4.6.5 Requirements for Time-Stamping of Records

CA archive records shall be automatically time-stamped as they are created. The CPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard.

4.6.6 Archive Collection System (Internal or External)

Archive data may be collected in any expedient manner.

4.6.7 Procedures to Obtain and Verify Archive Information

Procedures detailing how to create, verify, package, transmit, and store the CA archive information shall be published in the CPS.

4.7 KEY CHANGEOVER

To minimize risk from compromise of a CA’s private signing key, that key may be changed often. From that time on, only the new key will be used for certificate signing purposes. If the old private key is used to sign OCSP responder certificates or CRLs that contain certificates signed with that key, the old key must be retained and protected.

The CA’s signing key shall have a validity period as described in Section 6.3.2.

4.8 COMPROMISE AND DISASTER RECOVERY

The CA and directory system shall be deployed so as to provide 24-hour, 365-day availability. The CA shall implement features to provide high levels of reliability. The following subsections outline the policy for instances that may prevent such maintenance of reliability.

The CA shall have recovery procedures in place to reconstitute the CA within 72 hours in the event of a catastrophic failure, as described in the following subsections.

4.8.1 Computing Resources, Software, and/or Data are Corrupted

If the CA equipment is damaged or rendered inoperative, but the CA signature keys are not destroyed, CA operation shall be reestablished as quickly as possible, giving priority to the ability to generate certificate status information. The PA shall be notified as soon as possible.

4.8.2 CA Cannot Generate CRLs

If the CA cannot issue a CRL within 72 hours after the time specified in the next update field of its currently valid CRL, the PA shall be informed, as well as the Agency PMA(s) where appropriate.

4.8.3 CA Signature Keys are Compromised

In case of a CA key compromise, the PA shall be immediately informed, as well as any superior or cross-certified CAs. Subsequently, the CA installation shall be reestablished. If the CA distributes a trusted certificate for use as a trust anchor, the new self-signed certificate must be distributed via secure out-of-band mechanisms. The CPS shall detail the secure out-of-band mechanisms.

Subscriber certificates may be renewed automatically by the CA under the new key pair, or the CA may require subscribers to repeat the initial certificate application process.

4.8.4 Secure Facility Impaired after a Natural or Other Type of Disaster

In the case of a disaster whereby the CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, the PA shall be notified at the earliest feasible time, and the PA shall take whatever action it deems appropriate.

Relying parties may decide of their own volition whether to continue to use certificates signed with the destroyed private key pending reestablishment of CA operation with new certificates.

4.9 CA TERMINATION

In the event of termination of the CA operation, certificates signed by the CA shall be revoked. Prior to CA termination, the CA shall provide archived data to an archive facility as specified in the CPS. As soon as possible, the CA will advise all other organizations to which it has issued certificates of its termination, using an agreed-upon method of communication specified in the CPS.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 PHYSICAL CONTROLS

CA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. The CA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. CA cryptographic tokens shall be protected against theft, loss, and unauthorized use.

5.1.1 Site Location and Construction

The location and construction of the facility housing the CA equipment shall be consistent with facilities used to house high-value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorized access to the CA equipment and records.

5.1.2 Physical Access

At a minimum, the physical access controls shall—

- Ensure that no unauthorized access to the hardware is permitted
- Ensure that all removable media and paper containing sensitive plain-text information is stored in secure containers.
- Be manually or electronically monitored for unauthorized intrusion at all times
- Ensure an access log is maintained and inspected periodically
- Require two-person physical access control to both the cryptographic module and computer system

Removable cryptographic modules shall be inactivated before storage. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules, and CA equipment shall be placed in secure containers. Activation data shall be either memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.

A security check of the facility housing the CA equipment shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when “open,” and secured when “closed,” and for the CA, that all equipment other than the repository is shut down)
- Any security containers are properly secured
- Physical security systems (e.g., door locks, vent covers) are functioning properly
- The area is secured against unauthorized access.

A person or group of persons shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.3 Electrical Power

The CA shall have backup capability sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown. The directories (containing CA-issued certificates and CARLs) shall be provided with uninterrupted power sufficient for a minimum of 6 hours operation in the absence of commercial power, to maintain availability and avoid denial of service.

5.1.4 Water Exposures

CA equipment shall be installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors).

5.1.5 Fire Prevention and Protection

No stipulation.

5.1.6 Media Storage

Media shall be stored so as to protect them from accidental damage (e.g., water, fire, or electromagnetic). Media that contain audit, archive, or backup information shall be duplicated and stored in locations separate from the CAs.

5.1.7 Waste Disposal

Sensitive media and documentation that are no longer needed for operations shall be destroyed in the disposal process. For example, sensitive paper documentation shall be shredded, burned, or other wise rendered unrecoverable.

5.1.8 Offsite Backup

Full system backups, sufficient to recover from system failure, shall be made on a periodic schedule, described in a CA's CPS. Backups are to be performed and stored offsite not less than once per week. At least one full backup copy shall be stored at an offsite location (separate from CA equipment). Only the latest full backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible, or the integrity of the CA will be weakened. The functions performed in these roles form the basis of trust for the entire PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

The primary trusted roles defined this policy are Administrator, Officer, Auditor, and Operator. These four, somewhat abstract, roles are derived from roles identified in the CIMC Protection Profile developed by NIST and will be employed at both CA and RA locations as appropriate.

5.2.1.1 Administrator

The administrator role is responsible for—

- Installation, configuration, and maintenance of the CA hardware and software
- Establishing and maintaining CA system accounts
- Configuring certificate profiles or templates and audit parameters
- Generating and backing up CA keys.

Administrators do not issue certificates to subscribers.

5.2.1.2 Officer

The officer’s responsibility is to ensure the following functions occur according to the stipulations of this policy, that is—

- Registering new subscribers and requesting the issuance of certificates
- Verifying the identity of subscribers and the accuracy of information included in certificates
- Approving and executing the issuance of certificates
- Requesting, approving, and executing the revocation of certificates.

5.2.1.3 Auditor

The auditor role is responsible for—

- Reviewing, maintaining, and archiving audit logs
- Performing or overseeing internal compliance audits to ensure that the CA and associated RAs are operating in accordance with its CPS.

5.2.1.4 Operator

The operator role is responsible for the routine operation of the CA equipment and operations such as system backups and recovery, or changing recording media.

5.2.2 Separation of Roles

Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may only assume one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role. The CA software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and an Officer role, assume both the Administrator and Auditor roles, and assume both the Auditor and Officer roles. No individual shall have more than one identity.

5.2.3 Identification and Authentication For Each Role

An individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

5.3 PERSONNEL CONTROLS

5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and must be U.S. citizens. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the CA shall be set forth in the CPS.

5.3.2 Background Check Procedures

Background check procedures shall be described in the CPS and shall demonstrate that requirements set forth in Section 5.3.1 are met.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the CA shall receive comprehensive training. Training shall be conducted in the following areas:

- CA (or RA) security principles and mechanisms
- All PKI software versions in use on the CA (or RA) system
- All PKI duties they are expected to perform
- Disaster recovery and business continuity procedures
- Stipulations of this policy.

5.3.4 Retraining Frequency and Requirements

All individuals responsible for PKI roles shall be made aware of changes in the CA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions For Unauthorized Actions

The CA shall take appropriate administrative and disciplinary actions against personnel who have performed actions involving the CA or its RAs that are not authorized in this CP, CPSes, or other published procedures.

5.3.7 Contracting Personnel Requirements

See 5.3.1.

PKI vendors who provide any services shall establish procedures to ensure that any subcontractors perform in accordance with this policy and the CPS.

5.3.8 Documentation Supplied to Personnel

Documentation sufficient to define duties and procedures for each role shall be provided to the personnel filling that role.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

Cryptographic keying material used by CAs to sign certificates, CRLs or status information shall be generated in FIPS 140 validated cryptographic modules. For CAs that issue certificates under id-fpki-common-High, the module(s) shall meet or exceed Security Level 3. For CAs that do not issue certificates under id-fpki-common-High, the module(s) shall meet or exceed Security Level 2. Multiparty control is required for CA key pair generation, as specified in Section 6.2.2.

CA key pair generation must create a verifiable audit trail that the security requirements for procedures were followed. The audit trail must identify and document any failures or anomalies in the key generation process, and any corrective actions taken. The documentation of the procedure must be detailed enough to show that appropriate role separation was used.

6.1.1.2 Subscriber Key Pair Generation

Subscriber key pair generation may be performed by the subscriber, CA, or RA. If the CA or RA generates subscriber key pairs, the requirements for key pair delivery specified in Section 6.1.2 must also be met.

Key generation shall be performed using a FIPS approved method.

6.1.2 Private Key Delivery to Subscriber

If subscribers generate their own key pairs, then there is no need to deliver private keys, and this section does not apply.

When CAs or RAs generate keys on behalf of the Subscriber, then the private key must be delivered securely to the Subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements must be met:

- Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key after delivery of the private key to the Subscriber.
- The private key must be protected from activation, compromise, or modification during the delivery process.
- The Subscriber shall acknowledge receipt of the private key(s).
- Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers.
  - For hardware modules, accountability for the location and state of the module must be maintained until the Subscriber accepts possession of it.
  - For electronic delivery of private keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure channel.

The CA must maintain a record of the subscriber acknowledgement of receipt of the token.

6.1.3 Public Key Delivery to Certificate Issuer

Where key pairs are generated by the Subscriber or RA, the public key and the Subscriber's identity must be delivered securely to the CA for certificate issuance. The delivery mechanism shall bind the Subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it must be at least as strong as the CA keys used to sign the certificate.

6.1.4 CA Public Key Delivery to Relying Parties

When a CA updates its signature key pair, the CA shall distribute the new public key in a secure fashion. The new public key may be distributed in a self-signed certificate or in a key rollover certificate.

Self-signed certificates shall be conveyed to relying parties in a secure fashion to preclude substitution attacks. Acceptable methods for self-signed certificate delivery are:

- The CA loading a self-signed certificate onto tokens delivered to Relying Parties via secure mechanisms;
- Secure distribution of self-signed certificates through secure out-of-band mechanisms;
- Comparison of the hash of the self-signed certificate against a hash value made available via authenticated out-of-band sources (note that hashes posted in-band along with the certificate are not acceptable as an authentication mechanism); and
- Loading certificates from web sites secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded.

[Practice Note: Other methods that preclude substitution attacks may be considered acceptable.]

Key rollover certificates are signed with the CA's current private key, so secure distribution is not required. [Practice Note: To ensure the availability of the new public key, the key rollover certificates should be distributed using directories and other repositories.]

6.1.5 Key Sizes and Signature Algorithms

This CP requires use of RSA PKCS#1, RSA-PSS, or ECDSA signatures; additional restrictions on key sizes and hash algorithms are detailed below. Certificates issued under this policy shall contain RSA or elliptic curve public keys.

Practice Note: Future versions of this policy may specify additional FIPS-approved signature algorithms.

Trusted Certificates shall contain subject public keys of at least 2048 bits for RSA or 224 bits for elliptic curve, and be signed with the corresponding private key.

CAs that generate certificates and CRLs under this policy shall use signature keys of at least 1024 bits for RSA and 163 bits for elliptic curve algorithms. Certificates that expire on or after December 31, 2010 shall be generated with at least 2048 bit keys for RSA and 224 bit keys for elliptic curve algorithms.

CAs that generate certificates and CRLs under this policy shall use the SHA-1, SHA-224, or SHA-256 hash algorithm when generating digital signatures. RSA signatures on certificates and CRLs that expire on or after December 31, 2010 shall be generated using SHA-256. ECDSA signatures on certificates and CRLs that expire on or after December 31, 2010 shall be generated using SHA-224 or SHA-256, as appropriate for the key length.

End entity certificates issued under id-fpki-common-authentication, id-fpki-common-cardAuth, and id-fpki-common-device that expire before December 31, 2010 shall contain RSA public keys that are at least 1024 bits in length or elliptic curve keys that are at least 163 bits. End entity certificates issued under id-fpki-common-authentication, id-fpki-common-cardAuth, and id-fpki-common-device that expire on or after December 31, 2010 shall contain RSA public keys that are at least 2048 bits or elliptic curve keys that are at least 224 bits.

End entity certificates issued under id-fpki-common-policy, id-fpki-common-hardware, and id-fpki-common-High that expire before December 31, 2008 shall contain RSA public keys that are at least 1024 bits in length or elliptic curve keys that are at least 163 bits. End entity certificates issued under id-fpki-common-policy, id-fpki-common-hardware, and id-fpki-common-High that expire on or after December 31, 2008 shall contain RSA public keys that are at least 2048 bits or elliptic curve keys that are at least 224 bits.

Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum triple-DES or equivalent for the symmetric key, and at least 1024 bit RSA or 163 bit elliptic curve keys through December 31, 2008. Use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall require at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 2048 bit RSA or 224 bit elliptic curve keys after December 31, 2008.

6.1.6 Public Key Parameters Generation

Public key parameters shall always be generated and checked in accordance with the standard that defines the cryptographic algorithm in which the parameters are to be used. Public key parameters prescribed in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186-2.

6.1.7 Parameter Quality Checking

Parameter quality checking (including primarily testing for prime numbers) shall be performed in accordance with FIPS 186-2.

6.1.8 Hardware/Software Subscriber key generation

Validated software or hardware cryptographic modules shall be used to generate all subscriber key pairs, as well as pseudo-random numbers and parameters used in key pair generation. Any pseudo-random numbers used for key generation material shall be generated by a FIPS-approved method. Symmetric keys may be generated by means of either software or hardware mechanisms.

6.1.9 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The use of a specific key is constrained by the key usage extension in the X.509 certificate.

Public keys that are bound into human subscriber certificates shall be used only for signing or encrypting, but not both. Subscriber certificates that assert id-fpki-common-authentication or id-fpki-common-cardAuth shall only assert the *digitalSignature* bit. Other human subscriber certificates to be used for digital signatures shall assert the *digitalSignature* and *nonRepudiation* bits. Subscriber certificates that contain RSA public keys that are to be used for key transport shall assert the *keyEncipherment* bit. Subscriber certificates that contain elliptic curve public keys that are to be used for key agreement shall assert the *keyAgreement* bit.

Public keys that are bound into CA certificates shall be used only for signing certificates and status information (e.g., CRLs). CA certificates whose subject public key is to be used to verify other certificates shall assert the *keyCertSign* bit. CA certificates whose subject public key is to be used to verify CRLs shall assert the *cRLSign* bit. CA certificates whose subject public key is to be used to verify Online Certificate Status Protocol (OCSP) responses shall assert the *digitalSignature* and/or *nonRepudiation* bits.

Public keys that are bound into device certificates may be used for signing, encrypting, or both. Device certificates to be used for digital signatures (including authentication) shall assert the *digitalSignature* bit. Device certificates that contain RSA public keys that are to be used for key transport shall assert the *keyEncipherment* bit. Device certificates that contain elliptic curve public keys that are to be used for key agreement shall assert the *keyAgreement* bit. Device certificates shall not assert the *nonRepudiation* bit.

The *dataEncipherment*, *encipherOnly*, and *decipherOnly* bits shall not be asserted in certificates issued under this policy.

6.2 PRIVATE KEY PROTECTION

6.2.1 Standards for Cryptographic Module

The relevant standard for cryptographic modules is *Security Requirements for Cryptographic Modules* [FIPS 140-2]. The PA may determine that other comparable validation, certification, or verification standards are sufficient. The PA will publish these standards. Cryptographic modules shall be validated to a FIPS 140 level identified in this section, or validated, certified, or verified to requirements published by the PA.

CAs that issue certificates under id-fpki-common-High shall use a FIPS 140 Level 3 or higher validated hardware cryptographic module. CAs that do not issue certificates under id-fpki-common-High shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module. RAs shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module. Subscribers shall use a FIPS 140 Level 1 or higher validated cryptographic module for all cryptographic operations. Subscribers issued certificates under the hardware users policy (id-fpki-common-hardware), one of the authentication policies (id-fpki-common-authentication or id-fpki-common-cardAuth), or common High policy (id-fpki-common-High) shall use a FIPS 140 Level 2 or higher validated hardware cryptographic module for all private key operations.

6.2.2 Private Key Multiperson Control

A single person shall not be permitted to invoke the complete CA signature process or access any cryptomodule containing the complete CA private signing key. CA signature keys may be backed up only under two-person control. Access to CA signing keys backed up for disaster recovery shall be under at least two-person control. The names of the parties used for two-person control shall be maintained on a list that shall be made available for inspection during compliance audits.

6.2.3 Private Key Escrow

CA private keys are never escrowed.

Subscriber key management keys may be escrowed to provide key recovery. The method for this shall be described in the CA’s CPS.

Under no circumstances shall a subscriber signature key be held in trust by a third party.

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Private Signature Key

The CA private signature keys shall be backed up under the same multiperson control as the original signature key. All copies of the CA private signature key shall be accountable material, and protected in the same manner as the original. Backup procedures shall be included in the CA’s CPS.

6.2.4.2 Backup of Subscriber Private Keys

Subscriber private signature keys whose corresponding public key is contained in a certificate asserting the id-fpki-common-authentication, id-fpki-common-cardAuth, or id-fpki-common-High policy may not be backed up or copied.

Subscriber private signature keys whose corresponding public key is contained in a certificate that does not assert id-fpki-common-authentication, id-fpki-common-cardAuth, or id-fpki-common-High may be backed up or copied, but must be held in the subscriber’s control. Backed up subscriber private keys must be encrypted using a symmetric algorithm of consistent strength or stored in a cryptographic module validated at FIPS 140 Level 2.

6.2.5 Private Key Archival

CA private signature keys and subscriber private signatures keys shall not be archived. Subscriber key management keys may be escrowed to provide key recovery. The method for this shall be described in the CA’s CPS.

6.2.6 Private Key Entry Into Cryptographic Module

Subscriber keys shall be generated by and in a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport; private keys must never exist in plaintext form outside the cryptographic token boundary.

Private or symmetric keys used to encrypt other private keys for transport must be protected from disclosure.

6.2.7 Method of Activating Private Keys

For certificates issued under id-fpki-common-authentication, id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-High and id-fpki-common-devices, the subscriber must be authenticated to the cryptographic token before the activation of the associated private key(s). Acceptable means of authentication include but are not limited to pass-phrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

For certificates issued under id-fpki-common-cardAuth, subscriber authentication is not required to use the associated private key.

6.2.8 Methods of Deactivating Private Keys

Cryptographic modules that have been activated shall not be left unattended or otherwise available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure or automatically after a period of inactivity as defined in the applicable CPS. CA cryptographic modules shall be removed and stored in a secure container when not in use.

6.2.9 Method of Destroying Subscriber Private Keys

Private signature keys shall be destroyed when they are no longer needed or when the certificates to which they correspond expire or are revoked. This will likely be performed by executing a "zeroize" command. Physical destruction of hardware is not required.

To ensure future access to encrypted data, subscriber private key management keys should be secured in long term backups or archived.

6.3 GOOD PRACTICES REGARDING KEY-PAIR MANAGEMENT

6.3.1 Public Key Archival

The public key is archived as part of the certificate archival.

6.3.2 Usage Periods for the Public and Private Keys

The usage period for the Common Policy Root CA key pair is a maximum of 20 years.

For all other CAs operating under this policy, the usage period for a CA key pair is a maximum of ten years. The CA private key may be used to sign certificates for at most four years, but may be used to sign CRLs and OCSP Responder certificates for the entire usage period. All certificates signed by a specific CA key pair must expire before the end of that key pair's usage period.

Subscriber public keys in certificates that assert the id-PIV-content-signing OID in the extended key usage extension have a maximum usage period of eight years. The private keys corresponding to the public keys in these certificates have a maximum usage period of three years.

All other subscriber public keys have a maximum usage period of three years. Subscriber signature private keys have the same usage period as their corresponding public key. The usage period for subscriber key management private keys is not restricted.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

CA activation data may be user-selected (by each of the multiple parties holding that activation data). If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

RA and Subscriber activation data may be user-selected. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

6.4.2 Activation Data Protection

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data should be either biometric in nature or memorized (not written down). If written down, activation data shall be physically secured or encrypted under a FIPS approved cryptographic algorithm, and shall not be stored with the cryptographic module.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

Computer security controls are required to ensure CA/RA operations are performed as specified in this policy. The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards**:**

- Require authenticated logins
- Provide Discretionary Access Control
- Provide a security audit capability
- Restrict access control to CA services and PKI roles
- Enforce separation of duties for PKI roles
- Require identification and authentication of PKI roles and associated identities
- Prohibit object reuse or require separation for CA random access memory
- Require use of cryptography for session communication and database security
- Archive CA history and audit data
- Require self-test security-related CA services
- Require a trusted path for identification of PKI roles and associated identities
- Require a recovery mechanism for keys and the CA system
- Enforce domain integrity boundaries for security-critical processes.

When CA equipment is hosted on evaluated platforms in support of computer security assurance requirements, the system (hardware, software, operating system) shall, when possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version of the computer operating system as that which received the evaluation rating.

6.6 LIFE-CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

The System Development Controls for the CA and RA are as follows:

- The CA shall use software that has been designed and developed under a formal, documented development methodology.
- Hardware and software procured to operate the CA shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the vendor cannot identify the PKI component that will be installed on a particular device).
- Hardware and software developed specifically for the CA shall be developed in a controlled environment, and the development process shall be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.
- The CA hardware and software shall be dedicated to performing one task: the CA. There shall be no other applications, hardware devices, network connections, or component software installed that are not parts of the CA operation. Where the CA operation supports multiple CAs, the hardware platform can support multiple CAs.
- Proper care shall be taken to prevent malicious software from being loaded onto the CA equipment. Only applications required to perform the operation of the CA shall be obtained from sources authorized by local policy. RA hardware and software shall be scanned for malicious code on first use and periodically thereafter.
- Hardware and software updates shall be purchased or developed in the same manner as original equipment, and shall be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the CA system, in addition to any modifications and upgrades, shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the software or configuration. The CA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use. The CA shall periodically verify the integrity of the software as specified in the CPS.

6.6.3 Life-Cycle Security Ratings

No stipulation.

6.7 NETWORK SECURITY CONTROLS

A network guard, firewall, or filtering router must protect network access to CA equipment. The network guard, firewall, or filtering router shall limit services allowed to and from the CA equipment to those required to perform CA functions.

Protection of CA equipment shall be provided against known network attacks. All unused network ports and services shall be turned off. Any network software present on the CA equipment shall be necessary to the functioning of the CA application.

Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment.

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

Requirements for cryptographic modules are as stated above in Section 6.2

7. CERTIFICATE AND CARL/CRL PROFILES

7.1 CERTIFICATE PROFILE

Certificates issued by a CA under this policy shall conform to either the Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile [FPKI-PROF] or the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program [CCP-PROF].

7.1.1 Version Numbers

The CA shall issue X.509 v3 certificates (populate version field with integer “2”).

7.1.2 Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions are defined in profiles. These profiles are written to prescribe an appropriate amount of control over an infrastructure yet be flexible enough to meet the needs of the various CAs and communities. PKIs issuing certificates asserting this CP shall comply with RFC 3280. Whenever private extensions are used, they shall be identified in a CPS. Critical private extensions shall be interoperable in their intended community of use.

7.1.3 Algorithm Object Identifiers

Certificates issued under this CP shall use the following OIDs for signatures:

sha1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
RSA with PSS padding	id-RSASSA-PSS ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10}
ecdsa-with-SHA1	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) 1}
ecdsa-with-SHA224	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 1}
ecdsa-with-SHA256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2}

The PSS padding scheme OID is independent of the hash algorithm; the hash algorithm is specified as a parameter (for details, see [PKCS#1]). Certificates issued under this CP must use the SHA-256 hash algorithm when generating RSA-PSS signatures. The following OID shall be used to specify the hash in an RSA-PSS digital signature:

SHA-256	id-sha256 ::= {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1}

Certificates issued under this CP shall use the following OIDs to identify the algorithm associated with the subject key:

RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1}

Where the certificate contains an elliptic curve public key, the parameters shall be specified as one of the following named curves:

ansip192r1	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 1}
ansit163k1	{iso(1) identified-organization(3) certicom(132) curve(0) 1}
ansit163r2	{iso(1) identified-organization(3) certicom(132) curve(0) 15}
ansip224r1	{iso(1) identified-organization(3) certicom(132) curve(0) 33}
ansit233k1	{iso(1) identified-organization(3) certicom(132) curve(0) 26}
ansit233r1	{iso(1) identified-organization(3) certicom(132) curve(0) 27}
ansip256r1	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7}
ansit283k1	{iso(1) identified-organization(3) certicom(132) curve(0) 16}
ansit283r1	{iso(1) identified-organization(3) certicom(132) curve(0) 17}

7.1.4 Name Forms

The subject field in certificates issued under id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-High, and id-fpki-common-device of the base certificate shall be populated with an X.500 Distinguished Name, with the attribute type as further constrained by RFC 3280.

The issuer field of certificates issued under the policies in this document shall be populated with an X.500 Distinguished Name, with the attribute type as further constrained by RFC 3280.

The subject alternative name extension shall be present and include the pivFASC-N name type in certificates issued under id-fpki-common-authentication and id-fpki-common-cardAuth.

7.1.5 Name Constraints

The CAs may assert name constraints in CA certificates.

7.1.6 Certificate Policies Extension

Certificates issued under this CP shall assert one of the following OIDs in the certificate policies extension, as appropriate:

id-fpki-common-policy ::= {2 16 840 1 101 3 2 1 3 6}
id-fpki-common-hardware ::= {2 16 840 1 101 3 2 1 3 7}
id-fpki-common-devices ::= {2 16 840 1 101 3 2 1 3 8}
id-fpki-common-authentication ::= {2 16 840 1 101 3 2 1 3 13}
id-fpki-common-High ::= {2 16 840 1 101 3 2 1 3 16}
id-fpki-common-cardAuth ::= {2 16 840 1 101 3 2 1 3 17}

7.1.7 Usage of Policy Constraints Extension

The CAs may assert policy constraints in CA certificates.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this CP shall not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Certificates issued under this policy shall not contain a critical certificate policy extension.

7.1.10 Key Usage Constraints for id-fpki-common-authentication

Certificates asserting id-fpki-common-authentication or id-fpki-common-cardAuth must include a critical keyusage extension, asserting only digitalSignature value.

7.2 CRL PROFILE

CRLs issued by a CA under this policy shall conform to the CRL Profile specified in [CCP-PROF].

7.2.1 Version Numbers

The CAs shall issue X.509 Version two (2) CRLs.

7.2.2 CARL and CRL Entry Extensions

Detailed CRL profiles addressing the use of each extension are specified in [CCP-PROF].

8. SPECIFICATION ADMINISTRATION

8.1 SPECIFICATION CHANGE PROCEDURES

The PA shall review this CP at least once every year. Corrections, updates, or suggested changes to this CP shall be publicly available. Suggested changes to this CP shall be communicated to the contact in Section 1.4; such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

8.2 PUBLICATION AND NOTIFICATION POLICIES

This CP and any subsequent changes shall be made publicly available within 1week of approval.

8.3 CPS APPROVAL PROCEDURES

The PA shall make the determination that a CPS complies with this policy. The CA and RA must meet all requirements of an approved CPS before commencing operations. In some cases, the PA may require the additional approval of an authorized agency. The PA will make this determination based on the nature of the system function, the type of communications, or the operating environment.

8.4 WAIVERS

The PA will not issue waivers; CAs issuing under this policy are required to meet all facets of the policy.

9. BIBLIOGRAPHY

The following documents were used in part to develop this CP:

ABADSG Digital Signature Guidelines, 1996-08-01 http://www.abanet.org/scitech/ec/isc/dsgfree.html

CCP-PROF X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program. http://www.cio.gov/ficc/documents/CertCRLprofileForCP.pdf

E-Auth E-Authentication Guidance for Federal Agencies, M-04-04, December 16, 2003.

FIPS 112 Password Usage, 1985-05-30 http://csrc.nist.gov/fips/

FIPS 140-2 Security Requirements for Cryptographic Modules, 1994-02 http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

FIPS 186 Digital Signature Standard (DSS), FIPS 186-2, January 27, 2000. http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf

FIPS 201 Personal Identity Verification (PIV) of Federal Employees and Contractors, FIPS 201, February 25, 2005. http://csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf

FOIACT 5 U.S.C. 552, Freedom of Information Act Http://www4.law.cornell.edu/uscode/5/552.html

FPKI-PROF Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile. http://csrc.nist.gov/pki/twg/y2000/papers/twg-00-18.xls http://www.cio.gov/fpkipa/documents/fpki_certificate_profile.pdf

ISO9594-8 Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 2000.

ITMRA 40 U.S.C. 1452, Information Technology Management Reform Act of 1996 Http://www4.law.cornell.edu/uscode/40/1452.html

NAG69C Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999

NSD42 National Policy for the Security of National Security Telecom and Information Systems, 5 July 1990 Http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt (redacted version)

NS4005 NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997

NS4009 NSTISSI 4009, National Information Systems Security Glossary, January 1999

PACS *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems*, Version 2.2, The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group, July 27, 2004. http://smart.gov/information/TIG_SCEPACS_v2.2.pdf

PKCS#1 Jakob Jonsson and Burt Kaliski, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, RFC 3447, February 2003.

PKCS#12 PKCS 12 v1.0: Personal Information Exchange Syntax, June 24, 1999 ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf

RFC 2510 Certificate Management Protocol, Adams and Farrell, March 1999

RFC 2527 Certificate Policy and Certificate Practices Framework, Chokhani and Ford, March 1999

RFC 2560 X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol – OCSP, Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin, and Carlisle Adams, June 1999.

RFC 3280 Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Housley et al., April 2002.

USGold GOVERNMENTWIDE DIRECTORY SUPPORT 2
TECHNICAL SERIES: The Updated USGold Schema, July 14, 1997.

10. ACRONYMS AND ABBREVIATIONS

CA	Certification Authority
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Object Registry
DN	Distinguished Name
DSS	Digital Signature Standard
FAR	Federal Acquisition Regulations
FASC-N	Federal Agency Smart Credential Number
FBCA	Federal Bridge Certification Authority
FIPS	(U.S.) Federal Information Processing Standard
FPKI	Federal Public Key Infrastructure
CCP-Prof	X.509 Certificate and CRL Extensions Profile for the Common Policy
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
MOA	Memorandum of Agreement (as used in the context of this CP, between an Agency and the PA allowing interoperation between two separate organizational CAs)
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Federal PKI Policy Authority
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)

SHA-1	Secure Hash Algorithm, Version 1
S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Sockets Layer
U.S.C.	United States Code
WWW	World Wide Web

11. GLOSSARY

Access

Ability to make use of any information system (IS) resource. [NS4009]

Access Control

Process of granting access to IS resources only to authorized users, programs, processes, or other systems. [NS4009]

Accreditation

Formal declaration by a Designated Approving Authority that an IS is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009]

Activation Data

Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).

Agency

Any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Executive Branch of the Federal Government.

Applicant

The subscriber is sometimes also called an “applicant” after applying to a CA for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]

Archive

Long-term, physically separate storage.

Audit

Independent review and examination of records and activities to assess the adequacy of system controls; to ensure compliance with established policies and operational procedures; and to recommend necessary changes in controls, policies, or procedures. [NS4009]

Audit Data

Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009audit trail]

Authenticate

To confirm the identity of an entity when that identity is presented.

Authentication

Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual’s authorization to receive specific categories of information. [NS4009]

Backup

Copy of files and programs made to facilitate recovery if necessary. [NS4009]

Binding

Process of associating two related elements of information. [NS4009]

Biometric

A physical characteristic of a human being, including a photograph for visual identification. For the purposes of this document, biometrics do not include handwritten signatures.

Certificate

A digital representation of information which at least (1) identifies the CA issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the CA issuing it. [ABADSG]. As used in this CP, the term "Certificate" refers to certificates that expressly reference the OID of this CP in the "Certificate Policies" field of an X.509 v.3 certificate.

Certification Authority (CA)

An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs.

Certification Authority Revocation List (CARL)

A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates that have been revoked.

CA Facility

The collection of equipment, personnel, procedures, and structures that are used by a CA to perform certificate issuance and revocation.

Certification Authority Software

Key Management and cryptographic software used to manage certificates issued to subscribers.

Certificate Policy (CP)

A specialized form of administrative policy tuned to electronic transactions performed during certificate management. A CP addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery, and administration of digital certificates. Indirectly, a CP can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

Certification Practice Statement (CPS)

A statement of the practices that a CA employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP or requirements specified in a contract for services).

Certificate-Related Information

Information, such as a subscriber's postal address, that is not included in a certificate. A CA managing certificates may use this information.

Certificate Revocation List (CRL)

A list maintained by a CA of the certificates it has issued that are revoked prior to their stated expiration date.

Certificate Status Authority

A trusted entity that provides online verification to a relying party of a subject certificate's trustworthiness and may also provide additional attribute information for the subject certificate.

Client (application)

A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.

Common Criteria

A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.

Component Private Key

Private key associated with a function of the certificate-issuing equipment, as opposed to being associated with an operator or administrator.

Compromise

Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]

Computer Security Objects Registry (CSOR)

Computer Security Objects Registry operated by NIST.

Confidentiality

Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]

Cross-Certificate

A certificate used to establish a trust relationship between two CAs.

Cryptographic Module

The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS 1401]

Cryptoperiod

Time span during which each key setting remains in effect. [NS4009]

Data Integrity

Assurance that the data are unchanged from creation to reception.

Digital Signature

The result of a transformation of a message by means of a cryptographic system using keys such that a relying party can determine (1) whether the transformation was created using the private key that corresponds to the public key in the signer’s digital certificate and (2) whether the message has been altered since the transformation was made.

Discretionary Access Control

Means of restricting access to objects based on user identity.

Duration

A field within a certificate that is composed of two subfields: “date of issue” and “date of next issue.”

E-Commerce

The use of network technology (especially the Internet) to buy or sell goods and services.

Employee

Any person employed by an Agency as defined above.

Encrypted Network

A network that is protected from outside access by NSA-approved high-grade (Type I) cryptography. Examples are Secure Internet Protocol Routing Network (SIPRNET) and TOP SECRET networks.

Encryption Certificate

A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions or to establish or exchange a session key for these same purposes.

End Entity

Relying parties and subscribers.

Federal Bridge Certification Authority (FBCA)

The FBCA consists of a collection of PKI components (Certificate Authorities, Directories, Certificate Policies, and Certificate Practice Statements) that are used to provide peer-to-peer interoperability among Federal Agency CAs.

Firewall

Gateway that limits access between networks in accordance with local security policy. [NS4009]

Information System Security Officer (ISSO)

Person responsible to the Designated Approving Authority for ensuring the security of an IS throughout its life-cycle, from design through disposal. [NS4009]

Inside Threat

An entity with authorized access that has the potential to harm an IS through destruction, disclosure, modification of data, and/or denial of service.

Integrity

Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.

Intellectual Property

Useful artistic, technical, and/or industrial information, knowledge, or ideas that convey ownership and control of tangible or virtual usage and/or representation.

Key Escrow

A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber’s private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [Adapted from ABADSG, “Commercial key escrow service”].

Key Exchange

The process of exchanging public keys in order to establish secure communications.

Key Generation Material

Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.

Key Pair

Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key and (2) even knowing one key, it is computationally infeasible to discover the other key.

Local Registration Authority (LRA)

An RA with responsibility for a local community.

Memorandum of Agreement (MOA)
An agreement between an organization and the PA allowing interoperation between two separate organizational CAs.

Mission Support Information
Information that is important to the support of deployed and contingency forces.

Mutual Authentication
Authentication when parties at both ends of a communication activity authenticate each other (see “Authentication”).

Naming Authority
An organizational entity responsible for assigning DNs and for assuring that each DN is meaningful and unique within its domain.

National Security System
Any telecommunications or information system operated by the U.S. Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA]

Nonrepudiation
Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender’s identity so that neither can later deny having processed the data. [NS4009]. Technical nonrepudiation refers to the assurance a relying party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal nonrepudiation refers to how well possession or control of the private signature key can be established.

Object Identifier (OID)
A specialized formatted number that is registered with an internationally recognized standards organization; the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI OIDs are used to uniquely identify each of the policies and cryptographic algorithms supported.

Out-of-Band
Communication between parties using a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).

Outside Threat
An unauthorized entity from outside the domain perimeter that has the potential to harm an IS through destruction, disclosure, modification of data, and/or denial of service.

Physically Isolated Network
A network that is not connected to entities or systems outside a physically controlled space.

PKI Sponsor
Fills the role of a subscriber for nonhuman system components that are named as public key certificate subjects and is responsible for meeting the obligations of subscribers as defined throughout this CP.

Privacy
Restricting access to subscriber or relying party information in accordance with Federal law and Agency policy.

Private Key
(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair used to decrypt confidential information. In both cases, this key must be kept secret.

Public Key
(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair used to encrypt confidential information. In both cases, this key is made publicly available, normally in the form of a digital certificate.

Public Key Infrastructure (PKI)
A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Registration Authority (RA)
An entity that is responsible for identification and authentication of certificate subjects but does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of an authorized CA).

Re-key (a certificate)
To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.

Relying Party
A person or Agency who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate and is in a position to rely on them.

Renew (a certificate)
The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.

Repository
A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.

Responsible Individual
A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.

Revoke a Certificate
To prematurely end the operational period of a certificate effective at a specific date and time.

Risk
An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Risk Tolerance

The level of risk an entity is willing to assume in order to achieve a potential desired result.

Root CA

In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.

Secret Key

A "shared secret" used in symmetric cryptography, wherein users are authenticated based on a password, PIN, or other information shared between the user and the remote host or server. A single key is shared between two parties: the sender, to encrypt a transmission, and the recipient, to decrypt the transmission, with the shared key being generated with an algorithm agreed to beforehand by the transacting parties.

Server

A system entity that provides a service in response to requests from clients.

Signature Certificate

A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.

Subscriber

A subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device.

System Equipment Configuration

A comprehensive accounting of all system hardware and software types and settings.

System High

The highest security level supported by an IS. [NS4009]

Technical Nonrepudiation

The contribution of public key mechanisms to the provision of technical evidence supporting a nonrepudiation security service.

Threat

Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]

Trust List

Collection of trusted certificates used by relying parties to authenticate other certificates.

Trusted Agent

Entity authorized to act as a representative of an Agency in confirming subscriber identification during the registration process. Trusted Agents do not have automated interfaces with CAs.

Trusted Certificate

A certificate that is trusted by the relying party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor."

Trusted Timestamp
A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.

Trustworthy System
Computer hardware, software and procedures that (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.

Two-Person Control
Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements. [NS4009]

Update (a certificate)
The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.

Zeroize
A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS 1401]